

The next 6 lines of text, shows us,how a valid configuration file swtorssh.cfg should looks like.

fullssh.sh	ssh-id	Compress	4	2	22	9999	NoShell	username1@dnsname.server.de	xxxxx	xxxxxx	Germany	my-home-server-wan
fullssh.sh	ssh-id	Compress	4	2	22	9999	clock	username1@10.0.0.66	xxxxx	xxxxxx	Germany	my-home-server-lan
fullssh.sh	ssh-id	xxxxxxx	4	2	22	9999	Noshell	username2@127.124.166.21	xxxxx	backup	Austria	freds-server
fullssh.sh	passwd	Compress	4	1	443	9999	Noshell	hjfdj@84.55.22.166	xxxxx	xxxxxx	France	french-pgp-server
chainssh.sh	ssh-id	Compress	4	2	22	9999	chain	username1@dnsname.server.de	11000	xxxxxx	Canada	mychain1.cfg
chainssh.sh	ssh-id	Compress	4	2	22	9999	chain	ujdfhj1@188.67.88.15	11000	xxxxxx	Poland	mychain2.cfg

This help file describes the syntax for the configuration file

~/Persistent/swtor-addon-to-tails/swtorcfg/swtorssh.cfg

This settings are all valid with version 0.39 or higher.

- Every possible ssh-connection is defined in one single line.
- There is no limitation of ssh-servers, that can be defined.
- Every ssh server could be defined with a valid ipv4 address or a user friendly dns-name.
- All configuration parameters inside the configuration file swtorssh.cfg are case sensitive.
- There are 13 columns possible for every ssh-connection. All 13 fields have to be filled out !
- Spaces " " inside the of the fields 12 and 13 are not supported ! Every space " " has to be replaced with a "-".

Column 1:

This column 1 has 3 possible entry's → [fullssh.sh] [chainssh.sh] [pfssh.sh]
Only one of them, can be chosen.

fullssh.sh

This the best possible option for a ssh-connection. In this case we have somewhere a ssh account without any restrictions or borders for our own actions.

- A login over password or ssh-id is possible.
- We have enough space to store some backups on that ssh-server.
- We have a unrestricted shell to use like /bin/bash.
- We could use the commands scp or sshfs to transfer files to the remote ssh-host.
- We could even start a remote X11 applications over the ssh-tunnel like xclock or a browser.

chainssh.sh

A few ssh-servers on the internet don't like direct connection attempts made from over the onion-network.
If we would like to connecting to such a onion unfriendly ssh-server, we have to first masquerade our origin ip with a first ssh server in place,acting as a jump-server. You have to connect to the jump Server first and from over there without any password to the second ssh-server itself.

tails -> onion-network Nodes 1,2,3 -> ssh-connection > JUMP-SERVER -> ssh-connection -> DESTINATION-SERVER

This scenario is bit tricky to accomplish, because of the following reasons.

- The DESTINATION-SERVER has to support a pass-wordless login
- There are at least 2 different public/private ssh keys involved.
- Column 11 on the same line contains the second part to use with our ssh-command to the first server.

pfssh.sh

This kind of shell-account is very limited in the usage in general. As a little example, who offer this kind of a limited ssh-access accounts, you may have a look on this following website.

<http://www.dewassh.net/server/SSH>

- Only a simple port-forwarding is allowed, nothing more than this simple task can be done.
- No other shell than the good old "jail" called /bin/false is usable over this ssh connection.
- A login is only possible with a valid password. Logins over a public/private key are not possible or even desired.
- The ssh-logins has a expiration time between 3 and 30 days. After the expiration of the account, you have to create a new one.
- Some providers have a large base of country's to choose from where the ssh-server should be came from.
- Some silly ssh-providers only allow the creation of a ssh-account with a valid facebook or google+ account. Of course we don't give them away our credentials for facebook or google+.

Column 2:

This column 2 has 2 possible entry's → [ssh-id] [passwd]
Only one of them, can be chosen.

ssh-id

If we have a private/public key generated for a ssh-connection, we can use this public key stored inside ~/.ssh as a replacement for a password-less login to the remote server.

passwd

Every time we connect to this ssh-server, we have to provide a valid password.
The password will be send over to the remote ssh-server with sshpass. The password for this session is not stored on the persistent volume. It will be asked in a dialog-box on every startup of the ssh-connection.

Column 3:

This column 3 has 2 possible entry's → [Compress] [xxxxxxx]
Only one of them, can be chosen.

Compress

By default compression is not enabled for any outgoing ssh connections on any linux system. Very simple compression is no problem for modern CPUs and even on a gigabit network it is faster to compress data first before sending it over the network instead of leaving it uncompressed. This options tells the scripts that we would like to use Compression in our specific ssh-connection. On the ssh command-line this would be the option -C.

xxxxxxx

In the case that no Compression should be used, this dummy text has to be used.

Column 4:

This column 4 has 1 possible entry → [4]

Tails only supports tcp ip version 4.

Column 5:

This column 5 has 2 possible entry's → [2] [1]
Only one of them, can be chosen.

There are only 2 ssh protocols available to use inside of ssh. Most users should write a 2 here.
Only use the old ssh protocol version 1,if you know exactly, what you are doing !

<http://www.snailbook.com/faq/ssh-1-vs-2.auto.html>

Column 6:

This column 6 has only one possible entry → [22]

It defines the remote tcp port of the ssh-server we would like to connecting. The standard port for a ssh server is 22. This port information may can be something different than 22.

Column 7:

This column 7 has only one possible entry → [9999]

This value describes the port to build our socks5 server. The only possible value is 9999. You could change this value if you would like to change it, but this predefined port 9999 is hard encoded into all the scripts. Do change this value to something other than 9999 only, if you know what you are exactly doing !

Column 8:

This column 8 has 3 possible entry's → [NoShell] [clock] [chain]
Only one of them, can be chosen.

NoShell

After a successful login we could normally start a remote shell on the foreign ssh-server. Because we are in no need to use a classic shell after the login this option is used. On a linux server that shell would be normally /bin/bash. Please remember to write exactly NoShell and not NOSHELL or Noshell.

clock

Almost every ssh server can make use of the X11-window system. If the statement clock is found here, a nice clock like the following one as example

<http://tclock.sourceforge.net/tclock-shot.gif>

is displayed as soon we are connected to our ssh server. This option clock needs a fullssh.sh connection inside of the field 01. The displayed clock shows the current time of the remote ssh-server.

chain

With this option it is possible to build a "JUMP-SERVER" configuration. This special keyword is mandatory, because we need to connect to a second ssh-server after successful login on the first server.

Column 9:

This column 9 has only one possible entry → username@server

The data provided here, containing the username and the host-server we would like to connecting over ssh.
A possible entry of this field with a dns server-name:

username1@dnsname.server.com

or a the same entry with a ip instead of a dns-name :

username1@177.56.43.3

Column 10:

This column 10 has 2 possible entry's → [xxxxxx] [11000]
Only one of them, can be chosen.

xxxxxx

Almost all users can write this dummy text xxxxx here.

11000

This single value here written in this field can be in the range of
1024 until 65535. A value here is only valid in the main mode "chainssh.sh" of field 01,
we need this value as second port definition.

Column 11:

This column 11 has 2 possible entry's → [xxxxxx] [backup]
Only one of them, can be chosen.

xxxxxx

Almost all users can write this dummy text xxxxx here.

backup

If you have multiple ssh-servers to chose from, with this column 11, you can set exactly one of this ssh-server from the list as a predefined backup-server. Multiple backup statements inside of the configuration file swtorssh.cfg are not supported by now. In a later release it will be possible to encrypt the backups. By now, the backups made with my scripts are just simply compressed tar.gz files. You should save this sensitive backups only to a ssh-host that you can trust at 100 %.

Column 12:

This column 12 describe the county, that our ssh-server is located. Please write a single "-" instead of a single space " " if your complete country-name contains spaces inside of the name.

United Kingdom will be to ->United-Kingdom
Dominican Republic will be -> Dominican-Republic

Of course if we are using the mode "chainssh.sh" we do provide the country where our server2 is located.

Column 13:

This column 13 is a description field for most users with one exception, if you are using chainmode.ssh. Like in the country field 12 write a single "-" instead of single space " " inside of the text as description.

my-home-server-wan
my-home-server-lan

In the main mode "chainssh.sh" only, we use this description field to make our second connection. We need to create a new .cfg file for every chainmode.sh connection, we would like to use inside of the addon. If Columns 13 contains the value mychain1.cfg. You should create a file called mychain1.cfg inside of the directory ~/Persistent/swtor-addon-to-tails/swtorcfg. In this example we could write the following single command inside this configuration file mychain1.cfg

ssh -AtC42N -D11000 [fs-username1@war.freeshells.org](https://www.freeshells.org)

This command will be executed on our "JUMP-SERVER" to make the ssh-connection to the Destination server.

- A Enables forwarding of the authentication agent connection
- t Force pseudo-terminal allocation
- C Requests compression of all data
- 4 only use tcp version 4
- 2 Use only ssh 2 protocol
- N Do not execute a remote command. This is useful for just forwarding ports.
- D Specifies a local "dynamic" application-level port forwarding

Note : -D11000 must be made, according the port definition inside the value of column 10.
Numbers below of 1023 can not be used,because only root can use thisport numbers.